

## 多段 NAT 環境における通信最適化の検討

藤崎智宏<sup>††</sup> 松本存史<sup>†</sup> 加藤朗<sup>††</sup>

IPv4 アドレスの在庫枯渇が目前に迫っており、対応が急務である。長期的な対応策としては IPv6 の導入が挙げられるが、既存の IPv4 インターネットの延命も必要となる。延命策としては、ISP レベルでの LSN (Large Scale NAT) の導入が想定される。ISP レベルに NAT が設置されると、ユーザ宅内に NAT がある場合には、NAT が多段になることになり、効率的な通信が阻害されるか場合がある。本稿では、多段 NAT 環境における問題点を指摘し、通信の最適化手法を提案する。

### Optimizing communications under multiple NATs environment

Tomohiro Fujisaki<sup>††</sup> Arifumi Matsumoto<sup>†</sup> and Akira Kato<sup>††</sup>

Today, the Internet is widely used in varied ways, and lots of devices are connected. Because of this expansion of the Internet, IPv4 address will run out in a few years, and countermeasures are discussed in all over the world. Solution of this address run out will be to introduce next generation Internet Protocol, IPv6, however, it will take some time and need to expand the IPv4 lifetime. Introducing provider level NAT is one solution, however, there will be many problems to implement NAT in the ISP network. In this paper, we describe some problems to deploy ISP level NATs, and propose efficient IPv4 communication optimization technique in the multiple NATs environment.

### 1. はじめに

インターネットの基幹プロトコルである IPv4 は、32 ビット幅のアドレス空間によりおよそ 43 億個のアドレス数を持つが、インターネットの発展に伴い、IPv4 アドレス在庫の枯渇が問題になってきている。この IPv4 アドレス在庫枯渇に関する問題は、1990 年始め頃より議論が開始され、短期的解決として CIDR(Classless Inter-Domain Routing) の導入によるアドレス利用効率の向上が図られ、これは速やかに実装され普及した。しかしながら、その後も爆発的なインターネットの利用拡大は進み、IPv4 アドレスの在庫枯渇は目前に迫っている。この問題に対して、全世界レベルでの対策が急がれている。日本でも、多くの業界団体からなる組織である IPv4 枯渇対策タスクフォースにて対応策が検討されており[1]、長期的な対応策としては、IPv4 の後継として標準化された IPv6[2]の導入が必要とされているが、中・短期的な対応策として、IPv4 の延命を図ることが必要とされている。IPv4 の延命策としては ISP 網内に Network Address Translator (NAT)を導入し、グローバル IPv4 アドレスを複数ユーザで共有することにより IPv4 アドレスの消費量を抑える手法が有力である。しかしながら、ISP 網内に NAT を設置する場合、ユーザ宅には既に NAT が設置されていることがあるため、通信経路途中で NAT が多段に存在する「多段 NAT 環境」となる可能性がある。この「多段 NAT 環境」では、いくつかの問題が発生することが知られている。本稿では、「多段 NAT 環境」で発生する問題点のうち、ISP 網内で同じ NAT 下に属するユーザ同士の通信が、NAT での折り返しになってしまい、経路が冗長になってしまう点について、その解決策を提案する。第二章では、IPv4 アドレスの管理構造、IPv4 アドレス利用の現状、及び、アドレス在庫枯渇への対応策について述べる。第三章では、IPv4 アドレス在庫枯渇の対応策として提案されている、ISP レベルの NAT 導入モデルについて説明し、その問題点として、特に通信の非効率性について述べる。第四章にて通信の最適化手法を提案し、複数の実装形態を提示、それぞれの特徴を述べる。第五章にてまとめと、今後の課題について述べる。

### 2. IPv4 アドレス在庫枯渇とその対応

#### 2.1 IPv4 アドレス利用の現状

IP アドレスや AS 番号などのインターネット資源は IANA (Internet Assigned Numbers Authority)が全世界的に一元管理しており、これらの資源の分配を下位組織である地域レジストリ (RIR: Regional Internet Registries) に委譲している。地域レジストリでは、

<sup>†</sup> 日本電信電話株式会社  
Nippon Telegraph and Telephone Corporation

<sup>††</sup> 慶應義塾大学大学院  
Keio University Graduate School of Media Design

各地域の ISP（ローカルインターネットレジストリ）からの IP アドレス要求に対して、審査の上、必要量を割り振っている。世界的なインターネットの拡大を受け、IPv4 アドレスの需要が非常に高まっており、その枯渇は急速に減少している。図 1 に、インターネット資源管理団体である APNIC (Asia Pacific Network Information Centre) のチーフサイエンティストである Geoff Huston 氏が提供している IPv4 アドレス在庫枯渇予測のグラフを示す。Huston 氏の 2009 年 9 月 9 日時点の予測によると、IANA における IPv4 アドレスの在庫は 2011 年 8 月になくなり、続いて地域レジストリにおいても 2012 年 6 月に ISP に渡す IP アドレスがなくなる、としている（この予測はアドレ

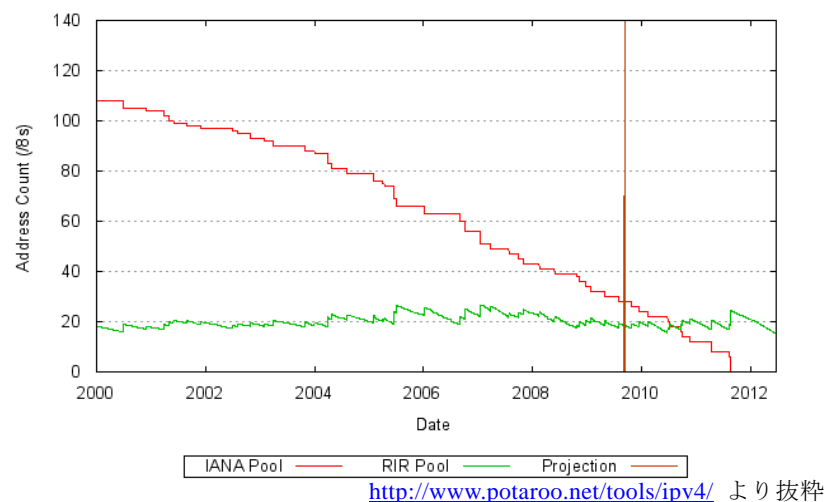


図 1 IPv4 アドレスの枯渇予測

スの使用状況をリアルタイムに反映し、日々更新されている[3])。

## 2.2 IPv4 アドレス在庫枯渇への対応

未割り当ての IPv4 アドレス空間の減少に伴い、世界各地で IPv4 アドレス枯渇に対していかに対応するかが検討されている。日本においても、総務省が主導した研究会[4]、日本のアドレスレジストリである JPNIC (Japan Network Information Center) における枯渇対策検討[5]、前述の IPv4 枯渇対策タスクフォースなどで議論されており、対策として

1. NAT を利用した IPv4 アドレスの有効利用
2. 未使用/不要 IPv4 アドレスの回収、流通
3. IPv6 の導入

の 3 つが考えられている。このうち、1 は、NAT はユーザ側のみにはしか導入できないこと、ユーザ側に NAT を導入することで IPv4 グローバルアドレスの使用量は減少する可能性はあるが、依然として割り当ては続くこと、2 は、今後、どの程度の IPv4 アドレスが流通するか不明であり、必要などきに必要量の IPv4 アドレスが入手可能かわからないこと、また、不要なアドレスの回収に伴い、IPv4 アドレスが細分化され、IPv4 経路表のさらなる増大を招く可能性が高い、といった問題点が指摘されている。このため、IPv4 アドレス枯渇に対する唯一永続的な解としては 3 点目の IPv6 の導入のみであるが、現在の IPv6 の普及状況等から、IPv4 を極力延命し、その間に IPv6 の導入を進めていくことが必要であるとされている。

## 3. プロバイダレベル NAT の利用と問題点

2 章で述べたように、今後の IPv4 インターネットには、プロバイダレベルで NAT が導入されることが予想される。インターネットの標準化組織である IETF (Internet Engineering Task Force) においても、プロバイダレベルの NAT (LSN: Large Scale NAT<sup>a</sup>) の導入モデルが提案されている。

### 3.1 NAT 導入モデル

IETF にて議論されている現インターネットと親和性の高い IPv4 アドレス枯渇対応方式には、大別して NAT444 モデル[6]、NAT464 モデル (ds-lite モデル) [7]、A+P モデル[8] の 3 種類がある。それぞれの手法を図 2 に示す。図中、IPv4(G)は IPv4 グローバルアドレスを、IPv4(P)は、IPv4 プライベートアドレスの利用を示す。

#### 3.1.1 NAT444 モデル

既存の IPv4 ベースのネットワークにおいて、ISP 内に NAT を設置し、複数ユーザで IPv4 グローバルアドレスの共有を図る方式である。ユーザ設備（ユーザ宅内のブロードバンドルータや PC 等）の改変が必要ないことが利点であるが、ユーザ宅内に CPE（ブロードバンドルータ等）が設置されている場合、NAT が多段になり、アドレス変換が二度行われることになる。

#### 3.1.2 NAT464 モデル (ds-lite モデル)

ユーザ宅とプロバイダ間のネットワークを IPv6 化し、ユーザ宅内のブロードバンドルータと ISP 内に設置した NAT 装置 (ds-lite 対応) が協調することで、IPv4 インターネットへのアクセスを提供するモデルである[6]。プロバイダ側は IPv6 ネットワークのみでよいため、IPv6 ネットワークへの移行が進み、IPv6 がメインになった際に IPv6 ネットワークを利用して IPv4 を提供する方式と考えられる。現状でも、IPv6 網が存在する環境では利用可能な方式である。

<sup>a</sup>従来、プロバイダレベルの NAT は、CGN (Carrier Grade NAT) と呼ばれていたが、キャリアのみが導入するものでもないということから、LSN(Large Scale NAT)と改名されている。

### 3.1.3 A+P モデル

IPv4 を拡張し、アドレスとポートの一部を利用して機器を特定するようにすることで、実質的に利用可能な IPv4 アドレス数を増やす手法である。A+P のシステムは、プロバイダエッジと、ユーザ宅内 CPE から構成される。IPv4 グローバルアドレスとポートでユーザ宅が指定されるため、前述の NAT のモデルと違い、ポート範囲は限られるが従来の IPv4 と同じような利用が可能となる。ユーザ宅内の CPE、及び、プロバイダエッジ機器の改変が必要となるため、他の方式に比べ、既存設備への改変範囲が広がる。

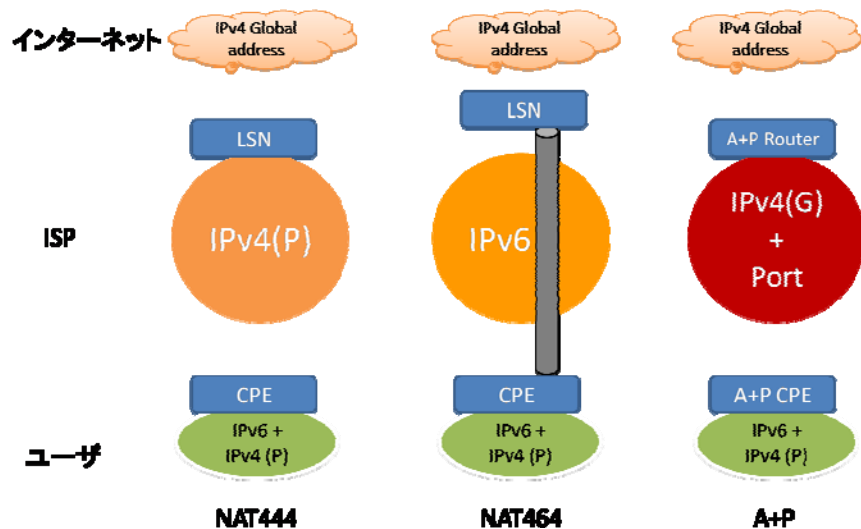


図 2 IPv4 アドレス枯渇期のネットワークモデル

### 3.2 多段 NAT の問題点

3.1.1 節で述べたように、ISP レベルに NAT を導入した場合、ユーザ宅内に NAT が存在する場合に多段 NAT の環境となる。NAT が多段に存在する環境では、以下のような問題点がある。

1. 少数の IP アドレスを複数ユーザで共有するため、ユーザが利用可能な通信セッション数に制限がある。一般的な TCP/IP 通信で使用される TCP のポート番号空間は 16 ビット長である。IPv4 アドレスの節約を考えた場合、一つの IPv4 グローバルアドレスをなるべく多くのユーザで共有することが必要であるが、この場合、一ユーザ当りで使用可能なポート数すなわち、利用可能な TCP セッション数に制限が発生し、この制限を超えた場合、通信が

できなくなる。

2. トラブルシューティングのために、変換のロギングをする場合、収容ユーザ数に応じ、ロギング情報が膨大になることが想定される。また、ユーザの特定のために記録が必要な情報も、IP アドレスと時刻のみでなく、ポート番号情報も追加して必要となる。また、いくつかの国においては、ユーザ特定のためにログ情報の保持が義務化されている。
3. IPv4 アドレスの利用効率を高めるためには、1 台の NAT 装置でなるべく多くのユーザをしゅうやくすることになる。集約度が大きくなると、NAT 装置の故障で影響を受ける範囲も広くなり、また、NAT 装置が single point of failure となる。
4. 従来、NAT の内部に設置された機器に対して、NAT を超えて通信するために、uPnP (Universal Plug & Play) や、NAT トラバースといったプロトコルが利用されている。これらの多くのプロトコルは、多段 NAT を想定していないため、NAT 外部からの通信が困難になる。
5. 多数のユーザが同一の IP アドレスを共有するため、サーバ側での対処が必要になる場合がある。例えば、ユーザを識別するためには IP アドレスのみでなく、ポートの情報も必要になる。また、ユーザが、同一アドレスを使用している前提で作成されているアプリケーション/システムの動作に問題が発生する (例: PoP before SMTP など)。
6. 現状、ユーザは家庭内にて RFC1918 で規定されているプライベートアドレス空間を利用している。ISP の LSN 配下で、同様のアドレスを使用する場合、ユーザの利用しているプライベートアドレス空間と競合が発生する可能性がある。
7. 同一 NAT 配下のユーザ同士の通信が、NAT 装置経由になる(ヘアピンング)ため、通信が非効率となる。

1,2 の問題については、NAT の仕組みに起因する問題であり、根本的な解決は困難である。IPv6 への移行を促進し、NAT の利用を減らす等の対策が必要である。3 については、NAT の内部変換テーブルまで含めた冗長構成を取ることが可能な NAT 装置を導入することで対処が可能であり、LSN の要件のひとつとすることが提案されている [西谷さんドラフト]。4 に関しては、uPnP にかわる新たなプロトコルを策定すること等で対応できる可能性もあるが、ISP 網内の NAT 装置をユーザ側から制御することになるため、他ユーザへの影響やセキュリティを考えた場合、実現は難しい。1,2 と同様、外部からの通信が必要なアプリケーションでは IPv6 を利用する等が望ましい。5 については、サーバ側での対処が必須となる。6 については、LSN 配下で利用する、ISP 専用プライベートアドレスの提案が実施されている [9]。7 については、アクセス網内の通信回線への影響や、NAT 機器の負荷、通信遅延の発生などの原因ともなる。

次章では、7の問題を詳説し、解決方法を提案する。

## 4. 多段 NAT 環境下における通信最適化

### 4.1 NAT 下における通信

図 4 に、NAT が多段になった場合のネットワーク構成を示す。プロバイダ内の LSN は、インターネットと通信する際のグローバル IPv4 アドレスを保有する。各家庭の CPE (Customer Premises Equipment, ブロードバンドルータ等) には、IPv4 プライベートアドレス、もしくは ISP が LSN 配下で利用する IPv4 アドレスが割り当てられる。家庭内部のホストが外部サーバと通信する場合、CPE、及び、プロバイダ内の LSN で始点アドレスの変換が二度実施されることになる。

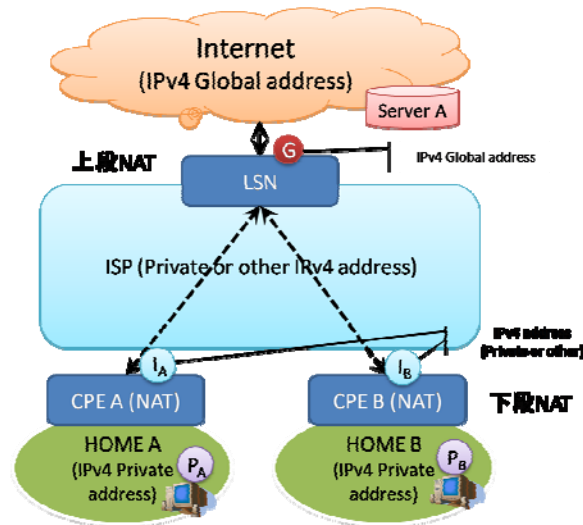


図 3 多段 NAT モデル

同じ LSN 下に属する家庭 (HOME A, HOME B) 内の機器が通信することを考える。従来の、CPE のみに NAT が存在する環境では、CPE に IPv4 グローバルアドレスが付与されるため、家庭内機器のアドレスとして CPE に付与された IPv4 グローバルアドレスが利用される。図 4 のように NAT が二段ある環境では、HOME B 内の機器に対するアドレスとして、LSN に付与された IPv4 グローバルアドレス G が利用されることが多い。これは、P2P ソフトウェアなど、通信相手の発見をインターネット上のサーバに依存するソフトウェアの場合には顕著である。このとき、IPv4 グローバルアド

レス G とポート番号の組み合わせと、CPE B のアドレス  $I_B$  とポート番号の組み合わせのマッピングが LSN に保持される。このように、同一の LSN 配下の通信装置同士の通信であっても、相手のアドレスとして変換後の IPv4 グローバルアドレスを指定するため、すべてのパケットが LSN を経由して行われることとなり、アクセスネットワークでの最適な経路制御が行われず非効率な通信となってしまう。

### 4.2 NAT 下通信の最適化

NAT が多段になっている環境における最適でない通信は、初段 NAT (CPE) が、通信相手が同一 LSN(上段 NAT)下に存在することを発見することで、LSN を介さない直接通信が可能となり、最適化できる。発見手法については、

1. LSN にて、通信の折り返しが発生した場合に、下段の NAT にアドレス/ポート番号情報を通知する。通知を受けた下段 NAT にて、通信最適化を実施する (受動的発見手法)。
2. 下段 NAT が、通信相手が同じ LSN 下にいることを自動的に発見し、通信の最適化を実施する (能動的発見手法)。

が考えられる。

#### 4.2.1 受動的発見手法

LSN (上段 NAT) では、折り返し通信が発生したことを検知することができる。LSN と、下段 NAT の間に、情報通知のプロトコルを定義し、上段 NAT から下段 NAT に、折り返し通信の発生をシグナリングする。通知を受けた下段 NAT にて、NAT の変換テーブルを操作し、通信先アドレスを変更することで通信の最適化を実施する。

HOME A 内の IPv4 プライベートアドレス  $P_A$  を持つノード A が、HOME B 内の IPv4 プライベートアドレス  $P_B$  を持つノード B と通信する場合を考える。ノード B は、自分のアドレスとして、IPv4 グローバルアドレス G と特定ポート番号を利用するものとし、LSN では、アドレス G の特定ポート番号 P 宛の通信を、アドレス  $I_B$  宛の通信としてアドレス変換し、CPE B に転送、CPE B では、その通信をアドレス  $P_B$  宛の通信として変換、ノード B に転送する設定が事前にされているものとする。以下、パケットの始点アドレス(src)、始点ポート(p1)、終点アドレス(dst)、終点ポート(p2)の組を、(src:p1, dst:p2) と表記することとする。

従来の通常通信は、

- ① ノード A は、ノード B 宛パケットとして ( $P_A:p1, G:P$ ) を送信。
- ② CPE A は、( $I_A:p1, G:P$ )として転送。
- ③ LSN は、( $G:p1, I_B:P$ ) と変換して CPE B 向けに転送。
- ④ CPE B では、( $G:p1, P_B:P$ ) と変換して、ノード B に転送。
- ⑤ ノード B では、返答を、( $P_B:P, G:p1$ ) として送信。

- ⑥ CPE B では、 $(I_B:P, G:p1)$ として転送.
  - ⑦ LSN では、 $(G:P, I_A:p1)$ と変換し、CPE A に転送.
  - ⑧ CPE A では、 $(G:P, P_A:p1)$ と変換し、ノード A に転送.
- となる. 3, 7 の処理が LSN での折り返し通信処理であり、以降の通信は LSN 経由となる. ここで、LSN が、最初に 3 の通信を発見した場合に、CPE A に対して折り返し通信の発生と、転送先を通知する. 最適化を含んだ転送シーケンスは図 4 のようになる.

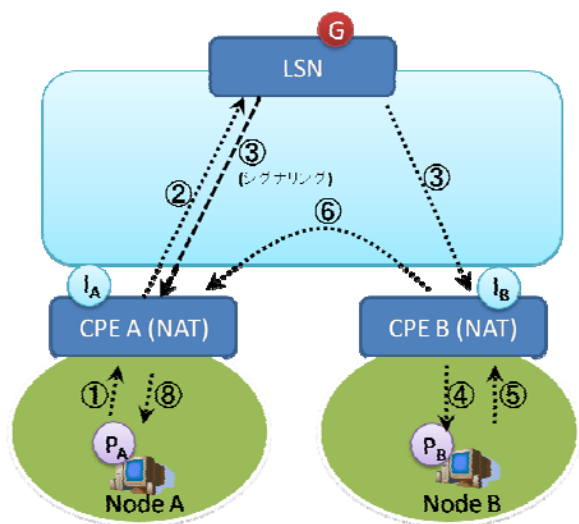


図 4 LSN からの情報通知による最適化

- ① ノード A は、ノード B 宛パケットとして  $(P_A:p1, G:P)$  を送信.
  - ② CPE A は、 $(I_A:p1, G:P)$ として転送.
  - ③ LSN は、上記パケットを受信後、CPE A に対して転送先アドレス  $I_B:P$  を通知し、最適化を指示. 最適化確認後、CPE B 向けに、 $(I_A:p1, I_B:P)$ として転送.
  - ④ CPE B では、 $(I_A:p1, P_B:P)$ と変換して、ノード B に転送.
  - ⑤ ノード B では、返答を、 $(P_B:P, I_A:p1)$ として送信.
  - ⑥ CPE B では、 $(I_B:P, I_A:p1)$ として転送.
  - ⑦ (LSN を経由しない).
  - ⑧ CPE A では、 $(P_B:P, P_A:p1)$ と変換し、C ノード A に転送
- これにより、以降の通信は LSN を経由せず、CPE A と CPE B 間の通信となる.

#### 4.2.2 能動的な手法

下段 NAT が通信開始の際に、LSN のアドレス変換処理によって失われない部分に、自身のアドレス情報、及びポート番号を付与する. 受信側では、アドレス情報が付与されていた場合、そのアドレスに対する通信を試みる. 通信が成立した場合には、以後、そのアドレスで通信する. このようにすることで、LSN からの情報がなくても、通信の最適化を実施することが可能である. 通信シーケンスは図 5 のようになる.

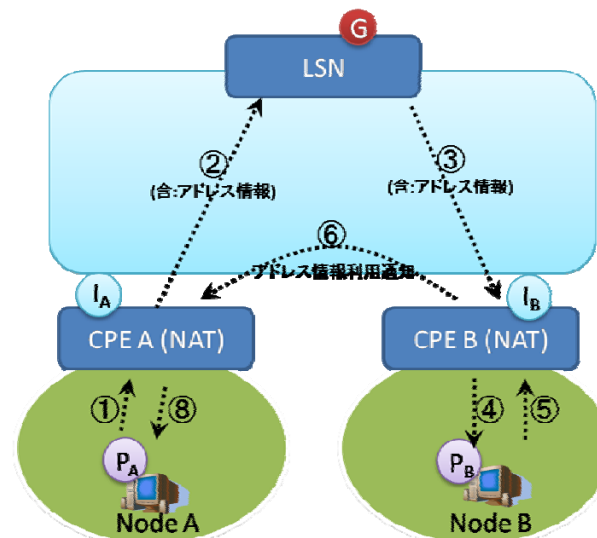


図 5 能動的な最適化

- ① ノード A は、ノード B 宛パケットとして  $(P_A:p1, G:P)$  を送信.
- ② CPE A は、 $(I_A:p1, G:P)$ として転送. 同時に、転送パケットに、CPE A 自身のアドレス情報、 $I_A:p1$  を付与する.
- ③ LSN は、 $(G:p1, I_B:P)$ と変換して CPE B 向けに転送. この際、CPE A が付与したアドレス情報には手を触れない.
- ④ CPE B では、アドレス情報、 $I_A:p1$  が付与されていることを発見、 $(I_A:p1, P_B:P)$ と変換して、ノード B に転送
- ⑤ ノード B では、返答を、 $(P_B:P, I_A:p1)$ として送信.
- ⑥ CPE B では、 $(I_B:P, I_A:p1)$ として転送. この際、付与されたアドレス情報  $I_A:p1$  を利用した旨を CPE A に通知.



- ⑦ (LSN を経由しない)
- ⑧ CPE A では CPE B からの通知に基づき、 $(P_A:p1, G:P) \rightarrow (I_A:p1, G:P)$  に関する NAT 変換テーブルを、 $(P_A:p1, G:P) \rightarrow (I_A:p1, I_B:P)$  と書き換え、受信パケットを  $(G:P, P_A:p1)$  と変換し、ノード A に転送

以降の通信は LSN を経由せず、CPE A と CPE B 間の通信となる。

CPE A が最初にパケットを送出する際に、CPE A 自身のアドレス情報を付加する方法、及び、CPE B が NAT テーブル変更要求を送る方法としては、IP オプションや TCP オプションを利用することが考えられる。

#### 4.2.3 セキュリティに関する考察

通信の最適化を実施する際には、通信パケットが他のノードにハイジャックされる等を防ぐ必要がある。“受動的発見手法”の場合には、LSN と CPE 間のシグナリングプロトコルにセキュリティを具備する、LSN と CPE 間であらかじめセキュリティ関係を確立しておく、等の手段が考えられる。“能動的発見手法”の場合には、通信を開始した機器 (CPE A) が受け取る NAT テーブル変更要求が、本当に通信相手からのものかを検証することが必須である。これには、最初に付加するアドレス情報に、認証データを同時に付与する等が考えられる。また、アドレスに関する情報の伝達範囲を狭めるために、LSN を通過して外部に出ていくパケットに対しては、LSN が CPE が付与した情報を削除する等が考えられる。

通知されたアドレス及びポート番号への NAT テーブル変更処理を、通知後十分時間が経ってから行うことによって、通信相手の送信元アドレスが不正なものではないことがある程度確認できる。例えば TCP の場合は 3 ウェイハンドシェイクが完了すれば、相手の送信元アドレスが詐称されていない可能性が高いため、この完了後にアドレスの切り替えを行う等により、セキュリティを高めることができる。

#### 4.2.4 両手法の評価

表 1 に、“受動的手法”と、“能動的手法”について、定性的な評価を述べる。

表 1 手法の評価

	変更点	通信時の処理	セキュリティ
受動的手法	LSN, CPE	影響なし	確保容易
能動的手法	CPE のみ	パケット MTU に影響	確保困難

既存設備から必要な変更点という観点では、“受動的手法”が、LSN と CPE の良能に変更が必要なことに対し、“能動的手法”では、基本的に CPE への変更のみが必要となる。通信時の処理に着目した場合、“受動的手法”では、実際に通信パケットに対して、アドレス変換以外の処理が発生しないが、“能動的手法”では、パケットに情報を

付加するため、通信 MTU の調整等が必要になる可能性がある。セキュリティという観点では、“受動的手法”では、NAT 変換テーブルの変更要求の送信元が、LSN のみであり、LSN がプロバイダ設備であることを考えると、送信元の認証を実施することは比較的容易かと思われる。一方、“能動的手法”では、NAT 変換テーブル変更要求の送信元が多数存在するため、要求メッセージが正当なものかどうかを確認するための仕組みが必要となる。

## 5. まとめと今後の課題

本稿では、多段 NAT 環境の問題を述べ、通信の非効率性を改称する通信最適化手法について提案し、定性的な評価を実施した。IPv4 アドレスの枯渇が近づくにつれ、プロバイダレベルの NAT 導入が増大していくことが想定されるため、本手法は有効であると考えられる。今後は、提案手法の評価をすすめ、また、実装して有効性を検証する。更に、現在のインターネットにおける折り返し通信量の測定データなどから、NAT 環境が導入された場合の NAT 下通信の割合を考察し、本手法がどの程度利用される可能性があるかについて検討を進める。

**謝辞** 通信最適化手法の議論にご協力いただいた、NTT 東日本の岩佐部長、水越部長に、謹んで感謝の意を表する。

## 参考文献

- 1) IPv4 アドレス枯渇対応タスクフォース, 「IPv4 アドレス枯渇対応アクションプラン 2009.2 版」, [http://www.kokatsu.jp/blog/ipv4/data/090217\\_v4exh\\_actionplan\\_jp.pdf](http://www.kokatsu.jp/blog/ipv4/data/090217_v4exh_actionplan_jp.pdf)
- 2) S. Deering, R. Hinden: Internet Protocol, Version 6 (IPv6) Specification., RFC2460, Dec. 1998.
- 3) IPv4 Address Report, <http://www.potaroo.net/tools/ipv4/>
- 4) 総務省, 「インターネットの円滑な IPv6 移行に関する調査研究会」, [http://www.soumu.go.jp/joho\\_tsusin/policyreports/chousa/ipv6/index.html](http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/ipv6/index.html)
- 5) JPNIC, 「IPv4 アドレス在庫枯渇問題に関する検討報告書(第一次)」, <http://www.nic.ad.jp/ja/ip/ipv4pool/ipv4exh-report-071207.pdf>
- 6) Y. Shirasaki, S. Miyakawa, A. Nakagawa, J. Yamaguchi and H. Ashida: NAT444 with ISP Shared Address, <http://tools.ietf.org/html/draft-shirasaki-nat444-isp-shared-addr>, Work in progress.
- 7) A. Durand et al: Dual-stack lite broadband deployments post IPv4 exhaustion, <http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite>, Work in progress.
- 8) R. Bush et al: The A+P Approach to the IPv4 Address Shortage, <http://tools.ietf.org/html/draft-ymbk-aplusp>, Work in progress.
- 9) Y. Shirasaki et al: ISP Shared Address, <http://tools.ietf.org/html/draft-shirasaki-isp-shared-addr>, Work in Progress.